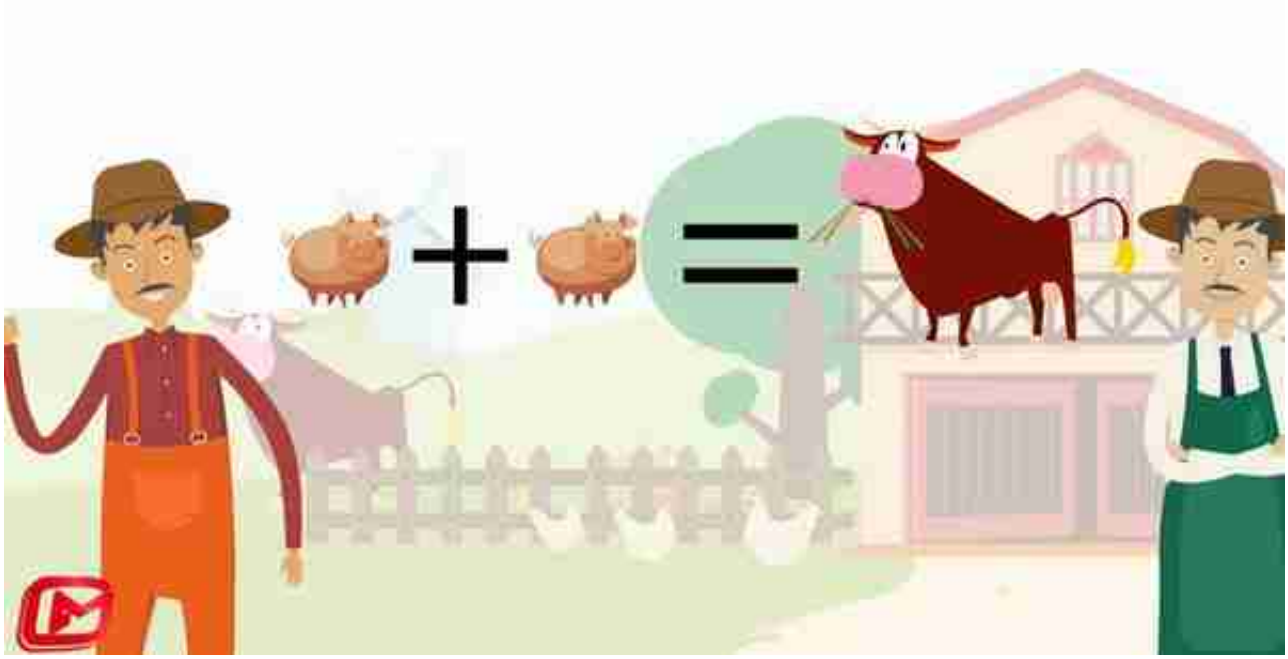
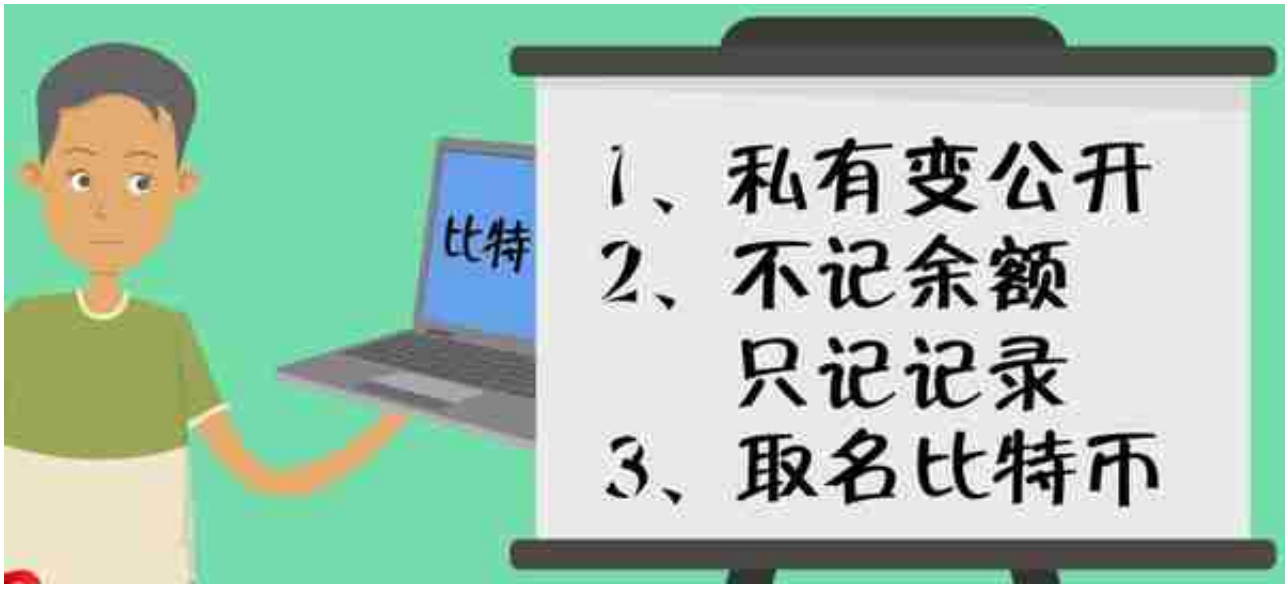
（为了方便大家阅读，这里贴出故事文字版，想看视频的朋友可以移步我的主页）



有一天，村民觉得这样太不方便了，于是村长组织全体村民召开大会，讨论如何解决这个问题，有人提议，我们可以将可以分割并且较为稀有的东西作为一般等价物，比如黄金，再把其他物品和黄金的重量关系编制成一张价格表，只要大家都认可，之后交易用黄金不就行了吗？村长觉得这个提议很好，便通过了提议，并且规定全村的黄金其他人都不可以采！只有村委会可以开采，然后根据大家的劳动量或者上缴的物资分配给大家。从此人们开始使用黄金买卖自己的物资。我们将这时的货币叫做“称量货币”。

过了一段时间，很多人开始抱怨自己家的纸币太多，总有丢失的事情发生。村长的儿子小村长很聪明，他对所有村民说：“我来找人记账，你们自愿把纸币放到我这里，以后交易的时候和我说一声，我直接在交易双方的账上进行增减，你们出门就可以不用带纸币拉！”村民很很高兴的同意了。于是中央系统虚拟货币诞生啦~也就相当于我们现在的银行。



此言一出，村民炸开了锅，不记录余额倒是可以理解，公开账本接受不了啊！谁都知道我有多少钱了啊！

中本聪说，别慌，我们这样来操作。为了隐私安全考虑，我们每个人都不用真实姓

名交易，我给每个人随机生成一个数，这个数介于0到2的256次方之间，出现的可能大概相当于宇宙中所有原子的数量，所以大家不用担心重复的问题。我再用一种固定算法（Base58）把这个数变成字符串，这个字符串就叫做私钥。你们自己一定保管好，私钥是你拥有比特币的唯一证明，也相当于你们的密码。

5KYZdUEo39z3FPrtuX2QbbwGnNP5zTd7yyr2SC1j299sBCnWjss

SHA256(SHA256(version + prev_hash + merkle_root + ntime + nbits + x)) < TARGET

大家可以通过改变X值来获取sha256函数结果，X可以是0-2的32次方之间的数，如果结果小于我们给定的目标值TARGET，我们就算他成功了。最直接的判断方法就是sha256函数得出的64位16进制数字的前若干位数均为0，（目前需要前18位均为0才算成功。）我们就奖励他50个比特币再加上你们转账的手续费。这里的每一页纸就叫做一个区块，整理账本的过程我们叫做打包区块，也就是俗称的挖矿。每一页连起来的账本就叫做区块链。

为了控制发行数量，我们规定将每十分钟内产生的交易记录写到一个区块上，然后让矿工们打包，最开始每打包一个区块奖励50比特币，之后每经过21万个区块（约4年时间）奖励就减半，直到2140年左右奖励不足时，大约一共发放2100万比特币。之后便不会再发放，那时矿工的奖励来源将是每笔交易的手续费。